Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

The Information Commissioner's Office (ICO) response to the Department for Business, Energy & Industrial Strategy's call for evidence on the UK's International Regulatory Cooperation Strategy

Questions 1-3 - About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003, amongst others.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

The ICO welcomes the opportunity to respond to this Department for Business, Energy & Industrial Strategy (BEIS) call for evidence on the UK's International Regulatory Cooperation Strategy. This response focuses on the ICO's involvement in international regulatory cooperation initiatives, work which is underpinned by the ICO's International Strategy.

Question 4: What international regulatory cooperation initiatives, if any, does your organisation undertake?
Please provide a comprehensive overview. This may include, for example, participation in international forums, membership of international networks, being involved in the development of international standards or instruments, formal cooperation with international organisations or counterparts (through a Memorandum of Understanding for example) and international enforcement initiatives. Note this list is not exhaustive.

The ICO is a lead and active participant in the following international networks:

- Global Privacy Assembly (GPA)
- International Enforcement Cooperation Working Group (IEWG)[1]
- Global Privacy Enforcement Network (GPEN)
- Council of Europe Committee of Convention 108
- OECD Working Party on Data Governance and Privacy in the Digital Economy

[1] IEWG is a permanent working group of the GPA.

- Conference of European Data Protection Authorities
- British, Irish and Islands' Data Protection Authorities network (BIIDPA)
- Common Thread Network (CTN)
- Unsolicited Communications Enforcement Network (UCENet)
- International Consumer Protection and Enforcement Network (ICPEN)

Lead roles

The Commissioner is currently Chair of the GPA; and the ICO co-chairs the IEWG with Canada (OPC) and US (FTC). The ICO also co-Chairs the CTN with Ghana (DPC) and is a Member of the GPEN Committee. The Deputy Commissioner (Executive Director, Regulatory Strategy) chairs the OECD Working Party. The ICO is a member of the UCENet Executive Committee.

Initiatives

International cooperation on enforcement and formal regulatory interventions are a key part of the ICO's toolbox to uphold UK individuals' data protection rights and hold organisations to account, allowing the ICO to regulate in a modern, cross-border economy. Indeed, working with regulatory partners across jurisdictions is essential in today's world where data knows no borders and innovations have global cross-regulatory implications.

We engage in key international networks (as outlined above) to establish and strengthen ties with regulatory partners in regions where enforcement cooperation is likely to be increasingly important due to emerging technologies and innovations that raise data protection concerns.

For example, through the ICO's co-Chair role of the GPA IEWG we drove support for a recent open letter[2] on increased privacy risks of video conferencing platforms as a result of massive uptake in use during the Covid-19 pandemic. Similarly, through the IEWG, ICO led discussion of concerns regarding Clearview AI – a facial recognition software company – and explored opportunities for joint working. Emerging from these early discussions, in July we announced a joint investigation with the Office of the Australian Information Commissioner (OAIC) into the company's use of 'scraped' data and biometrics of individuals[3].

The GPEN Committee organises an annual 'sweep' – an intelligence gathering operation – conducted by DPAs around the globe, focused on a specific issue.

[2] 21 July 2020 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/the-global-privacy-expectations-of-video-teleconference-providers/

[3] 9 July 2020 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc

Recent examples include looking at how well organisations have implemented the concept of privacy accountability into their own internal privacy programmes and policies (2018), and assessing user controls over personal information (2017). The results shed light on the issue at hand at a domestic level but also provide a useful point of comparison on the global scale.

We use Memoranda of Understanding (MoUs) to formalise cooperative relationships with key strategic partners around the world supporting joint work and information sharing on specific issues and cases. In other instances, we are able to rely on well-established relationships, although mindful that the relationships with EU counterparts will take on a different character after the end of the transition period.

The ICO has duties and functions to regulate several different information rights laws. Below is a summary of our key areas of international regulatory cooperation across the breadth of our regulatory activity:

Data Protection Act 2018 and General Data Protection Regulation (GDPR)

Investigations and complaints

The ICO coordinates complaint handling and investigations with other DPAs though mutual assistance and information sharing with partner DPAs via the GDPR's 'one stop shop' mechanism in the EU (until 31/12/20). The ICO has been the Lead Supervisory Authority (under Article 60) in a number of high profile cases, such as the BA and Marriott cases, which have required the penalty and action to be approved by the other EU DPAs. The agreed BA fine was announced in October 2020. For the Rest of the World, we use our participation in enforcement cooperation networks to cooperate on complaint handling and investigations – with the intention to replicate such arrangements with key EU DPAs after the end of the transition period.

Administrative decisions

In our assessment and approval of international transfer tools – BCRs in particular – we are currently subject to the GDPR's consistency mechanism, and engage and share information with relevant EU DPAs to ensure an effective process. Similar cooperation would be necessary in the development of transnational codes of conduct and EU level certification schemes under GDPR. Mutual recognition of such tools (or other arrangement) after the end of the transition period will be an item for consideration with the EU Commission.

Law enforcement

The ICO supervises UK use of EU law enforcement mechanisms and databases, through cooperation and coordination with EU DPAs. Such cooperation is limited during transition.

Policy development
We use our participation and leadership in various regional, cultural, and global DPA networks, and through bilateral relationships, to undertake soft engagement and influence to inform our own, and influence global, policy development on high standards and in key areas of data protection.

Privacy and Electronic Communications (EC Directive) Regulations 2003

The ICO engages in mutual assistance and intelligence sharing on complaints and issues around unsolicited communications with partner authorities in the EU via the Consumer Protection Network Cooperation System, and through global multilateral enforcement networks in RoW.

The Network and Information Systems Regulations (NIS) 2018

Through mutual assistance and information sharing, we cooperate with other competent authorities in the EU on investigations and enforcement activity in respect of cybersecurity incidents affecting digital service providers. This cooperation has been limited during transition.

Electronic Identification, Authentication and Trust Services Regulation (eIDAS)

The ICO cooperates with other supervisory bodies in the EU via the provision of mutual assistance, reporting on security breaches, and more general engagement on the harmonisation and effective regulation of trust services across the EU. This cooperation has been limited during transition.

Question 5: In your experience, what are the challenges for regulators, standards bodies and similar organisations in engaging in international regulatory cooperation initiatives?

Further to the challenges created by the UK's exit from the EU and subsequent loss of access to EU fora, as well as the ongoing uncertainty around the nature of any future negotiated relationship, we consider there to be four principal areas of challenge:

i. Increasing cross-regulatory nature of the digital economy (given digitalisation globally and its importance and impact on digital economies nationally and internationally).
ii. Limited scope (or clarity) within existing legislation to be able to share information.
iii. Remit and resources of our international counterparts, including in support of the extra-territorial application of (UK)GDPR.
iv. Cultural differences, both in legislation and approach.

We have provided more detail on each of these principal areas below:

i. <u>Increasing cross-regulatory nature of the digital economy</u>

Increasingly there is a recognised intersection between data protection, data security and privacy rights, and other sectors; for example, in the areas of online harms, use of algorithms and AI, consumer protection, competition, finance, and thus a need for regulators to interrogate data misuse and privacy rights access across the whole spectrum of the digital economy and collaborate to address systemic issues across different territories.

The desirability of working across regulatory frameworks associated with risk and harm is already recognised domestically in the development of the UK Regulators Network (UKRN) and Digital Regulation Cooperation Forum (DRCF).

For example, the DCRF was jointly formed by the ICO, the CMA and Ofcom to support regulatory co-ordination in the area of digital services, including issues with digital markets and online harms. This builds on existing bilateral and trilateral contacts between the three regulators (for example, in the CMA-led Digital Markets Taskforce). The DRCF was formally launched in July 2020. It is a non-statutory body, and does not attempt to supplant the statutory responsibilities of each regulator; rather, it is a voluntary coming together of the three regulators for communication and co-operation.

The DRCF has 6 objectives, which are broadly to do with promoting regulatory coherence, knowledge and resource sharing and promoting innovation. Joint work in some of these areas has started and we are developing the work plan for next year. One of the objectives relates to international work: objective 6 to strengthen international engagement with regulatory bodies to exchange information and share best practice regarding approaches to the regulation of digital markets.

This is an area where we are still developing our work plans, but it is one where we would look to leverage the international contacts that each regulator has in

their own sphere of activity. The ICO, for example, is involved in the GPA's Digital Citizen and Consumer Working Group, which is doing work on the intersection between DP and consumer and competition issues. We are aware that there are examples of regulators in other jurisdictions recognising their overlapping interests in regulating digital markets and beginning to co-operate, particularly in relation to competition and data protection issues. The DRCF represents a formalised but still voluntary form of this co-operation. We think it has potential to promote better regulation and better outcomes for citizens while recognising the importance of competition and innovation.

However, internationally the ability to work across regulatory frameworks is less developed (if at all, to our knowledge). See ii. below, also.

ii. <u>Limited scope (or clarity) within existing legislation to be able to share information</u>

There is an opportunity for legislation to be framed as an enabler for international cooperation and sharing. For example, Article 50 UKGDPR sets out the obligation for the Commissioner to cooperate internationally with third countries and international organisations 'for the protection of personal data'. The wording of clauses (a)-(c) however refers specifically to cooperation in the 'enforcement of legislation for the protection of personal data'. As such, although Article 50 does not limit cooperation to third country Data Protection Authorities (DPAs), neither does its wording explicitly enable cooperation with third country regulators in other sectors, given the reference to the ***enforcement of legislation for the protection of personal data***.

As an example, when working with consumer protection authorities internationally, the ICO may consider the privacy information provided to consumers or the privacy implications of a product being sold; however, we may also uncover information indicative of wider concerns, such as a fraud or scam, or a product safety issue. Such concerns fall outside of the ICO's remit and data protection legislation per se but nevertheless require action by another regulator or enforcement body in another jurisdiction (see i. above also). The ICO may consider it important to share this information and to cooperate with the other body in the interests of protecting UK data subjects. As it stands, Article 50 does not specifically enable this sort of information sharing and/or cooperation.

Similarly, s132 (DPA2018) is also relevant as it sets out the bases on which ICO can make lawful disclosures of information. Hitherto, s132 has arguably made it easier to share data with EU counterparts than with international or domestic institutions (e.g. on economic crime) on account of s132(2)(d) [disclosure necessary for discharge of an EU obligation]. This will be removed post transition

period. Beyond the parameters of the EU, the ICO has regularly relied on s132(2)(f) [necessary in the public interest] when sharing information. The concept of 'necessity' does not equate to 'desirability', thus potentially creating a barrier to data sharing that could be used for the public good.

iii. Remit and resources of our international counterparts, including in support of the extra-territorial application of (UK)GDPR.

The ICO is responsible for numerous pieces of legislation as outlined in our response to Question 3 above, which does not necessarily correlate with the competences of our counterpart data protection authorities (DPAs) internationally. This means we do not always have the necessary relationships or contacts to progress regulatory cooperation, or knowledge of who the appropriate regulator is. We are working to develop our international cooperation with non DPAs, for example through MoUs (Canadian Radio-television and Telecommunications Commission) and through our involvement in the Unsolicited Communications Enforcement Network (UCENet) and International Consumer Protection and Enforcement Network (ICPEN).

It can also be the case that regulators in third countries do not have the resource to pursue substantive cooperation activity. This may present an issue in the scenario where we are seeking to apply the extraterritorial scope of UK GDPR. It is highly likely that to do so successfully would require the cooperation of the data protection or privacy regulator within that third country.

iv. Cultural differences, both in legislation and approach

There are necessarily national variations in regulation and the grounds on which a third country can offer mutual assistance to the ICO and/or participate in a joint investigation. One international DPA, for example, did not feel comfortable in being a co-signatory to a recent open letter sent to VTC companies (coordinated by IEWG) on account of their legislation: sending a formal letter implied an obligation to investigate, which is not always desirable or the underlying intention of the intervention. In other cases, third country legislation may require data sharing with the UK to be done under the governance of their jurisdiction, which may be unfavourable to the ICO.

As our work within the EDPB has demonstrated, there can be differing legal interpretations of the (same) legislation which can hamper collaborative efforts. There may also be instances when relevant or salient information is shared with us by an international counterpart but there are restrictions on how it can be used (if at all) in progressing a domestic investigation. For example, we may not be able to use information provided in confidence where action may result in some or all of it being placed in the public domain via our normal processes, any

subsequent appeal and/or disclosure processes; and the UK has existing frameworks for dealing with covert evidence, or evidence obtained from a whistle-blower.

Question 6: How can the government support regulators, standards bodies and similar organisations in undertaking international regulatory cooperation through the development of a strategy?
For example, what guidance, information or training could be made available. Please also identify other ways that the government could provide support.

The ICO considers that the government could provide support in the following ways:

- Ensuring UK legislation is as enabling as it can be in encouraging and allowing regulatory cooperation, especially with respect to data sharing between sectors.
- Given the increasingly cross-cutting nature of regulation, development of a directory of domestic regulators to better understand the remit (and legislation) of each; this might also be used to identify shared regulatory interests.
- Further, such a directory could identify the international counterpart for each domestic regulator or piece of legislation.
- Identification of any UKRN equivalent in other countries in order to link comparable networks together ('network of networks'), and/or spearhead a proposal for a global equivalent of UKRN.
- Directory to also connect domestic regulators to the country desks at FCDO and in DIT (respectively).

Question 9: Please provide any views that might inform the government's international cooperation strategy.

There is an opportunity to promote effective cooperation by adopting mechanisms and an effective framework that enables participants to identify risk, harm and opportunity, arrive at policy positions, and, subsequently, follow a process that sets clear strategic priorities and objectives. These in turn should

drive and direct regulatory activities, including enforcement action either within or across networks, that can (collectively) be considered a truly international response to a particular issue(s) and for which the framework provides a mechanism to assess the impact of that response.

The ICO is happy to provide further input on these matters.

Information Commissioner's Office

November 2020